UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/890,286	07/27/2001	Mototsugu Nishioka	501.40397X00	3015

24956 7590 03/28/2005

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

4C

Office Action Summary	Application No.	Applicant(s)	
	09/890,286	NISHIOKA, MOTOTSUGU	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) *14-17* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☒ Claim(s) *1-5,7-10 and 12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 July 2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/890,286.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-17 have been examined. The applicant has cancelled claims 14-17. Claims 1-13 are still pending.

Priority

The examiner recognizes the applicant's claim to an earlier effective filing date of 1/29/1999 due to priority documents PCT/JP00/00475 and 11-021254.

Information Disclosure Statement

The IDS submitted by the applicant has been considered.

Specification

1. The abstract of the disclosure is objected to because there were two abstracts that were submitted on the same day and the examiner is unsure which one the applicant meant to be the one the examiner should consider. As such, the examiner has considered both abstracts. One abstract looks like it was submitted along with the rest of the specification and has the number 61 at the top of the page. For this one, on the last sentence, "are provided" should be changed to "is provided." The other abstract was submitted separately and looks like it's a copy of the front page of a PCT publication. This abstract is in an improper format and contains improper contents. If this was the abstract that the applicant meant for the examiner to consider, the applicant is reminded of the proper format and content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an

improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

Correction is required. See MPEP § 608.01(b).

2. On p3, line 24, "...be broken..." should be changed to "...can be broken...."

3. On p6, line 16, "is" should be removed.

4. On p7, lines 9-10, "...where k |pq|..." doesn't make sense. The examiner suggests

   "...k=|pq|...."

5. There were several places in the specification where subscripts or superscripts used in mathematical formulas were represented with fonts which were too small for the examiner to reasonably distinguish what the characters were. For instance, on p9 and p16, for the first two formulas, the examiner had a hard time determining what D is raised to; the applicant should consider using larger sized fonts to represent mathematical formulas.

6. On p12, line 14, "As the method..." should be "As for the method...."

7. On p13, line 12, "Keg" should be "Key."

8. On p13, line 19, "an" should be removed from the sentence.

9. Page 28, lines 7 and 12 refer to a Fig. 10. Fig. 10 does not exist. The examiner assumes the applicant meant Fig. 3.

10. On p35, line 4, "primer" should be "prime."

11. The examiner requires that the applicant submit the following NPL documents referenced in the specification for the examiner to be able to fully determine the patentability of the application: Reference documents 1, 3-6, and 8-12. See 37 CFR 1.105.

Claim Objections

Claims 1-5, 7-10, and 12 are objected to because of the following informalities:

1. The preamble of claim 1 refers to an encryption method, yet the method of decryption is also described. The examiner notes that later claims refer back to the decryption method mentioned in claim 1. The examiner would like to suggest the applicant move the text recited in claim 1 dealing with the decryption method to those claims dealing with decryption so as to avoid the problem of improper dependency which currently occur in those dependent claims.

2. Claims 2, 8, 9, 10, and 12 each have a similar problem as claim 1 in that the preamble refers to an encryption method, yet decryption is also described.

3. Claim 3 is objected to because on p3, line 2, "secrete" should be "secret."

4. Claims 4, 5, and 7 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. Claim 4 depends on claim 3 **and** claim 1. Claim 5 depends on claims 3 **and** 2.

Claim 7 depends on claims 6 **and** 2. See MPEP § 608.01(n). The examiner will attempt to apply art to the best of his understanding of these improperly dependent claims.

5. Claim 5, line 3 should say "...said sender composes...."

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al (US 6,141,420) in view of Maurer (US 5,150,411).

Claim 1:

Vanstone discloses that at the time the applicant's invention was made, a public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key (col 8, lines 20-31).

Vanstone does not explicitly disclose the public-key encryption method comprising the rest of what was recited in claim 1. However, what is disclosed by Vanstone reads on with the rest of what is recited in claim 1 for the most part. What Vanstone does not disclose at all deals with the additional data a which ensures that a ciphertext is uniquely decrypted to its plaintext.

Vanstone's invention deals with encryption based on elliptic curve algorithms (abstract). Elliptic curve encryption methods incorporated in public-key encryption algorithms which allows for reduced bandwidth and storage requirements were also disclosed as known at the time the applicant's invention was made (col 3, lines 39-42). It was also known by one of ordinary skill that the finite field defined by the points on an ellipsis defines a finite Abelian group. This is also disclosed by Vanstone (col 3, lines 60-63). As such, the public-key encryption method recited in claim 1 reads on the public-key encryption method which utilizes the properties of an elliptic curve disclosed by Vanstone except for the parts in claim 1 that was previously mentioned dealing with additional data a, which will now be addressed.

As mentioned, Vanstone does not disclose nor does Vanstone disclose anything that reads on the additional data a which ensures that a ciphertext is uniquely decrypted to its plaintext. However, Maurer discloses encryption in which additional data a, i.e. a Jacobi symbol, is calculated during an encryption process. Maurer discloses the Jacobi symbol as being important for defining a user's identity (and corresponding keys) in such a way as to achieve non-interactive secure transmission of messages (col 9, lines 44-52). This additional data a is used to calculate the ciphertext which gets sent. It would have been obvious for one of ordinary skill in the art at the time the applicant's invention was made to incorporate Maurer's teaching of a Jacobi symbol into Vanstone's teachings according to the limitations recited in claim 1 as it would allow for a public-key encryption method which achieves non-interactive secure transmission of messages. The Jacobi symbol would also ensures that a ciphertext is uniquely

decrypted to its plaintext because as mentioned, it is used to identify the sender whose key should be used to decrypt a message. Thus, the original plaintext m is calculated from the additional data a.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al (US 4,405,829) in view of Crepeau ("Computer Science 308-547A Cryptography and Data Security") and Vanstone et al (US 6,141,420).

Claim 2:

Rivest discloses a public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key comprising said public key, i.e. the well known RSA algorithm (col 6, lines 21-23).

Rivest also discloses other things which reads on a public-key encryption method comprising:

a) a key generation step which the receiver conducts by working the receiver-end device, according to a procedure comprising:

generating a secret key (p, q, s, β) consisting of elements p, q, s, and β where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$,
- $\beta \in Z$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$ and

generating a public key (n, g, h, k, l, α) consisting of elements n, g, h, k, l, and α (k is the bit length of pq) where:

- α, g, h, k, $l \in Z$ $(0<g, h<n)$

- n=p^(d)q (where d is an odd number).

b) An encryption step which the sender conducts by working the sender-end device, according to a procedure comprising:

- calculating equations (C and D) with regard to a plaintext m (0<m<2^(k-2)) and a random number r (0<=r<=1).
- composing a ciphertext (C,D) from the obtained C and D.
- sending the ciphertext (C,D) to said receiver.

Rivest discloses that p and q are prime numbers (col 4, lines 24-32). α and β disclosed by the applicant reads on e and d disclosed by Rivest (col 4, lines 21-23 and 67-68). Rivest's keys also have the property that $e*d \equiv 1 (\text{mod lcm } (p-1, q-1))$ as disclosed in col 13, line 1. This means that the type of cryptography used by both Rivest and the applicant is asymmetric cryptography. Equations C and D are read on by the disclosure in col 13, line 55-col 14, line 2 in which a message is encrypted to C and decrypted via D. These disclosures by Rivest reads on the limitations of claim 1 recited above including that of the public key generation as the public key must work with the secret key.

Further, Rivest also discloses that decoding may be performed modulo each of the prime factors and the results combined using "Chinese remaindering" or any equivalent method to obtain the result modulo (col 13, lines 31-34). This reads on the limitation recited in claim 1 dealing with the plaintext m (which was obtained from the ciphertext) any of which can be among ϕ(m (sub(1,p)), m(sub(1,q))), ϕ(-m (sub(1,p)), m(sub(1,q))), ϕ(m (sub(1,p)), -m(sub(1,q))), ϕ(-m (sub(1,p)), -m(sub(1,q))), where ϕ

represents ring isomorphism mapping from Z/(p)xZ(q) to Z/(pq) according to the Chinese remainder theorem and having to solve for equations m(sub(1,p)) and m(sub(1,q)).

Rivest do not teach an encryption step in which the sender calculates a Jacobi symbol a=(m/n) and anything recited in claim 2 dealing with a. However, Crepeau teaches computing a Jacobi symbol a=(m/n) (pages 5-6, section 1.5). Crepeau also teaches extracting square roots modulo p, which also reads on computing m(sub(1,p)) and m(sub(1,q)) (page 9, section 1.9).

Rivest and Crepeau do not teach s∈Z, gh^3≡1(mod pq). However, as mentioned in claim 1, Vanstone teaches elliptic curve encryption algorithms (abstract). It is known to one in the art of cryptography that if p and q are both primes and p is equal to q, then if there exists a finite group (G) of order pq, then G is an Abelian group, which implies the use of elliptic curve algorithms in the encryption method. As s is defined to be an integer such that the elements it is composed of (gh^3) is of order pq as defined by 1(mod pq), then this equation reads on the limitation recited dealing with elliptic curve algorithms. Note that g and h are also elements in the Abelian group. The examiner would also like to note that the user of elliptic curves in RSA cryptography is also well known in the art of cryptography at the time the applicant was made. It is also well known in the art that encryption using elliptic curves have the potential to provide for smaller key sizes and faster encryption.

It would have been obvious for one of ordinary skill in the art at the time the applicant's invention was made to combine Crepeau and Vanstone's teaching with

Rivest's teachings according to the limitations recited in claim 2. One of ordinary skills would have done so as it would have resulted in a cryptography method in which was faster than just using Rivest's method alone. Also, as mentioned in claim 1, the use of a Jacobi symbol would result in less resource needed for the cryptography method.

Claims 3 and 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al (US 4,405,829) in view of Crepeau ("Computer Science 308-547A Cryptography and Data Security"), Vanstone et al (US 6,141,420), and Schneier et al (US 6,091,835).

Claim 3:

Rivest, Crepeau, and Vanstone do not disclose said sender composes said plaintext m including check data for verifying the recovery of true information. However, the use of hashes/checksums for verification purposes was well known at the time the applicant's invention was made and also disclosed by Schneier (col 5, lines 11-15). It would have been obvious for one of ordinary skill in the art at the time the applicant's invention was made to modify the combination method of Rivest, Crepeau, and Vanstone in light of known information in the art and Schneier's teachings according to the limitation recited in claim 3. One of ordinary skill would have been motivated to do so as the use of a checksum would allow the integrity of the message to be checked once decrypted.

Claim 5:

Rivest, Crepeau, and Vanstone do not disclose a step that said sender composes said plaintext m including a predetermined redundant text in addition to a message text which must be transmitted to said receiver before encrypting the text in accordance with the procedure set forth in claim 2 and a step that said receiver verifies that the predetermined redundant text exists when performing decryption to recover the plaintext m in accordance with the procedure set forth in claim 2.

However, the use of hashes/checksums for verification purposes was well known at the time the applicant's invention was made and also disclosed by Schneier (col 5, lines 11-15). Hashes are computed from the data in the message itself, so in that regard is a predetermined redundant text. Schneier do not explicitly disclose the hash being transmitted to said receiver before encrypting the text in accordance with the procedure set forth in claim 2 and a step that said receiver verifies that the predetermined redundant text exists when performing decryption to recover the plaintext m in accordance with the procedure set forth in claim 2.

However, a hash computed from a plaintext must be computed from the plaintext before it is encrypted. Also, the choice of when to send the hash to the receiver is arbitrary as long as the receiver gets both the encrypted message and the hash at some point. The applicant's choice of sending the hash before encrypting the message does not patentably differentiate from Schneier's method of sending the hash and the encrypted message (col 8, lines 55-60). Schneier also discloses the receiver verifying the hash (col 8, lines 62-64), which reads on verifying that the redundant text exists when performing decryption to recover the plaintext m in accordance with the procedure

set forth in claim 2. It would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to modify Rivest, Crepeau, and Vanstone's combination method according to the limitations recited in claim 5 as it would have allowed for the use of hashes for verification purposes.

Claim 6:

Rivest, Crepeau, and Vanstone do not explicitly disclose the limitations recited in claim 6. However, Rivest discloses a cipher-feedback mode is used in some encoding/decoding devices (col 14, lines 12-19). Random functions that were made public are well known in the art even at the time the applicant's invention was made. Further, calculations for random number data point on an elliptical curve through the use of exclusive OR and data coherence are disclosed by Vanstone (col 13, lines 5-19).

It appears to the examiner that the limitations recited in claim 6 deals with creating a hash or checksum for the message and then encrypting the message along with the hash. Schneier discloses that using hashes for verification purposes was well known at the time the applicant's invention was made (col 5, lines 11-15). Further, hashes are usually created by using some sort of feedback mechanism as well as the exclusive OR function. As such, the limitations recited in claim 6, reads on the creation of hashed messages as disclosed by Schneier using the methods discloses by Rivest and Vanstone as known at the time the invention was made. It would have been obvious for one of ordinary skill to incorporate the teachings of Rivest, Vanstone, and Schneier according to the limitations recited in claim 6. One of ordinary skill would have done so as it would have allowed for a way to verify a message's integrity.

Claim 7:

Rivest, Crepeau, Vanstone, and Schneier do not explicitly disclose the limitations recited in claim 7. However, what they do disclose reads on the limitations recited in claim 7. Rivest discloses a public-key encryption and decryption method (abstract). Further, as mentioned in claim 6, the encryption method in claim 6 encrypts a message along with a hash of the message. The use of a hash for verification is disclosed by Schneier (col 5, lines 11-15). As claim 6 is dependent on claim 2, any message encrypted using the method disclosed in claim 6 can be decrypted using the decryption method set forth in claim 2 as the only thing which claim 6 adds to the encryption method is the hash and the encryption method is the same. Once the message is decrypted one of ordinary skill would likely use the hash to verify that the message was properly decrypted. One of ordinary skill would have to do this by calculating the hash of the message again using the same method set forth in claim 6. In light of these disclosures, it would have been obvious for one of ordinary skill to modify the combination method of Rivest, Crepeau, Vanstone, and Schneier according to the limitations recited in claim 7. One of ordinary skill would have done so for the same reason given in claim 6.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al (US 6,141,420) in view of Maurer (US 5,150,411) and Rivest et al (US 4,405,829) further in view of Crepeau ("Computer Science 308-547A Cryptography and Data Security") and Schneier et al (US 5,956,404).

Claim 4:

Vanstone, Maurer, Rivest, and Crepeau do not disclose a step that said sender composes said plaintext m including a predetermined redundant text in addition to a message text which must be transmitted to said receiver before encrypting the text in accordance with the procedure set forth in claim 1; and a step that said receiver verifies that the predetermined redundant text exists when performing decryption to recover the plaintext m in accordance with the procedure set forth in claim 1.

However, the use of hashes/checksums for verification purposes was well known at the time the applicant's invention was made and also disclosed by Schneier (col 5, lines 11-15). Hashes are computed from the data in the message itself, so in that regard is a predetermined redundant text. Schneier do not explicitly disclose the hash being transmitted to said receiver before encrypting the text in accordance with the procedure set forth in claim 1 and a step that said receiver verifies that the predetermined redundant text exists when performing decryption to recover the plaintext m in accordance with the procedure set forth in claim 1.

However, a hash computed from a plaintext must be computed from the plaintext before it is encrypted. Also, the choice of when to send the hash to the receiver is arbitrary as long as the receiver gets both the encrypted message and the hash at some point. The applicant's choice of sending the hash before encrypting the message does not patentably differentiate from Schneier's method of sending the hash and the encrypted message (col 8, lines 55-60). Schneier also discloses the receiver verifying the hash (col 8, lines 62-64), which reads on verifying that the redundant text exists

when performing decryption to recover the plaintext m in accordance with the procedure set forth in claim 1. It would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to modify Rivest, Crepeau, and Vanstone's combination method according to the limitations recited in claim 4 as it would have allowed for the use of hashes for verification purposes.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al (US 4,405,829) in view of Maurer (US 5,150,411).

Claim 8:

Rivest discloses a public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key (col 6, lines 21-23). The public key encryption method Rivest discloses reads on the limitations of claim 8 which comprises:

a. a key generation step which the receiver conducts by working the receiver-end device according to a procedure comprising:

generating a secret key (p, q, β) consisting of elements p, q, and β, where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$,
- $\beta \in Z$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$ (col 5, lines 5-10 and col 7, line 45-col 8, line 31)

and

generating a public key (n, k, α) consisting of elements n, k, and α (k is the bit length of pq), where:

- α, k$\in$Z,
- n=p^(d)q (where d is an odd number) (col 9, line 59-col 10, line 10);

b. encryption which the sender conducts by working the sender-end device (Fig 2), composing a ciphertext (col 7, line 65-col 8, line 5), and calculating the equation C = m(sub(1))^(2α) mod (n) (col 8, lines 33-38).

c. a decryption step which said receiver conducts by working said receiver-end device (Fig 2).

Rivest also discloses that decoding may be performed modulo each of the prime factors and the results combined using "Chinese remaindering" or any equivalent method to obtain the result modulo (col 13, lines 31-34). This reads on the limitation recited in claim 8 dealing with the plaintext m (which was obtained from the ciphertext) any of which can be among ϕ(m (sub(1,p)), m(sub(1,q))), ϕ(-m (sub(1,p)), m(sub(1,q))), ϕ(m (sub(1,p)), -m(sub(1,q))), ϕ(-m (sub(1,p)), -m(sub(1,q))), where ϕ represents ring isomorphism mapping from Z/(p)xZ(q) to Z/(pq) according to the Chinese remainder theorem and having to solve for equations m(sub(1,p)) and m(sub(1,q)).

Rivest does not disclose any of the recited limitations of claim 8 dealing with the Jacobi symbol a = (m(sub(1))/n) including the ciphertext being composed as a function of a and the calculation of m(sub(1)) in order to calculate a. However, Maurer discloses the use of a Jacobi symbol in the field of cryptography (col 9, lines 38-64). It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to modify Rivest's method in light of Maurer's teachings of a Jacobi symbol

such that it meets the limitations recited in claim 8. One of ordinary skill would have been motivated to do so for the same reason given in claim 1.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al (US 4,405,829) in view of Maurer (US 5,150,411) and Vanstone et al (US 6,141,420).

Claim 9:

Claim 9 is substantially similar to claim 8 except in claim 9, the secret key is also a function of the element s and the public key is also a function of the elements g, h, and I. As such, Rivest and Maurer reads on all the limitations recited in claim 9 that claim 9 has in common with claim 8. The limitations found in claim 9 that was not found in claim 8 and was not disclosed by Rivest and Maurer will now be addressed.

Claim 9 recites that the secret key (p, q, s, β) consists of elements p, q, s, and β, where s∈Z, gh^3≡1 (mod pq). However, as discussed in claim 2, this limitation as recited implies the use of an elliptic algorithm in the cryptography method as it implies a finite Abelian group. Note g, h, and I are also elements found in an Abelian group. As the secret key is based on an elliptic algorithm, the public key must also be based on an elliptic algorithm to properly work together to encrypt and decrypt a message. Vanstone discloses the use of elliptic algorithms in cryptography (abstract). It would have been obvious for one of ordinary skill in the art at the time the applicant's invention was made to combine the teachings of Rivest, Maurer, and Vanstone according to the limitations recited in claim 9. One of ordinary skills would have been motivated to do so for the as

the use of an elliptic algorithm in cryptography can lead to faster encryption and decryption.

Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et al (US 4,405,829) in view of Maurer (US 5,150,411) and Vanstone et al (US 6,141,420) further in view of applicant's disclosure of common knowledge in the field of cryptography.

Claim 10:

Claim 10 is a modification on claim 9. For any similarities claim 10 has with claim 9, the rejections used for claim 9 also apply to claim 10. The difference between the two claims is that claim 10 is modified to resist adaptive chosen ciphertext attacks as evident from the way C' and D' are calculated. This type of attack was disclosed by the applicant as known and ways of resisting such an attack were also known at the time the applicant's invention was made (specification, p3, lines 3-10). In light of applicant's disclosure of common knowledge at the time the applicant's invention was made, it would have been obvious for one of ordinary skill in the art to combine the teachings of Rivest, Maurer, Vanstone, and common knowledge in the art according to the limitations recited in claim 10. One of ordinary skill would have been motivated to do so to prevent attacks using adaptive chosen ciphertext techniques.

Claim 11:

Claim 11 recites steps necessary to prevent attacks using adaptive chosen ciphertext techniques. As such, it would have been obvious for one of ordinary skills to

further modify the method recited in claim 10 according to the limitations recited in claim 11 for the same reason given in claim 10.

Claim 12:

Claim 12 is substantially similar to claim 10 except in the way m(sub(1)) is obtained. As such, any limitations recited in claim 12 that was recited also in claim 10 are rejected for the same reasons given in claim 10. The difference between the two claims is that in claim 12, m(sub(1)) is calculated by just concatenating m with r (i.e. m(sub(1)) = m||r). It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to calculate m(sub(1)) in the manner recited in claim 12 instead of the manner recited in claim 10 as it would have allowed for a faster encryption method as the way in which m(sub(1)) is calculated in claim 12 is simpler than the one in claim 10.

Claim 13:

Claim 13 recites steps necessary to prevent attacks using adaptive chosen ciphertext techniques. As such, it would have been obvious for one of ordinary skills to further modify the method recited in claim 12 according to the limitations recited in claim 13 for the same reason given in claim 10.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

PP